Discrete Mathematics 78 (1989) 217–222
North-Holland

ON THE BAYS–LAMBOSSY THEOREM

Neal BRAND
Department of Mathematics, North Texas State University, Denton, Texas 76203, U.S.A.

Received 6 May 1987
Revised 1 December 1987

The Bays–Lambossy Theorem states that if p is a prime then any pair of cyclic isomorphic $t-(p, k, \lambda)$ designs are isomorphic by a multiplier map. For each prime, $p \equiv 1(6)$, and $n \geq 2$ this paper gives examples of cyclic $2-(p^n, 3, 1)$ designs (or Steiner triple systems) which are isomorphic but not isomorphic by any multiplier. These examples show that any generalization of the Bays–Lambossy theorem for the stated parameters would have to involve more than just multiplier maps.

1. Introduction

The Bays–Lambossy Theorem [1, 5] states that if p is a prime and if two cyclic $t-(p, k, \lambda)$ designs are isomorphic then they are isomorphic by a multiplier map. An open problem is to determine for which values of t, v, k and λ the theorem generalizes. In [2] examples of cyclic $2-(4^n, 3, 2)$ $(n \geq 2)$ designs are given which are isomorphic but not by any multiplier. On the other hand, in [3] geometric conditions are given for cyclic $2-(pq, 3, 2)$ designs with p and q distinct primes which imply that isomorphic designs are multiplier isomorphic. In this paper examples of isomorphic cyclic $2-(p^n, 3, 1)$ designs, or Steiner triple systems, with $p \equiv 1(6)$ a prime and $n \geq 2$ are given which are not isomorphic by any multiplier.

Some definitions and notation are given which will be used throughout. A cyclic design is a design with v-set Z_v, the cyclic group of order v, and $x \to x+1$ is a design automorphism. A multiplier is a map $Z_v \to Z_v$ given by $x \to mx$ for $m \in Z_v$ with $(m, v) = 1$. A difference family on Z_v is a collection of ordered triples, B, with entries in $Z_v - \{0\}$ having the properties that for all $x \in Z_v - \{0\}$ the number of triples in which x occurs plus the number of triples in which $-x$ occurs is a constant, λ, and the sum of each triple is 0. It follows that if $\mathcal{B}$ is a difference family then $\tilde{\mathcal{B}} = \{\{x, x+a, x+a+b\} \mid x \in Z_v, (a, b, c) \in \mathcal{B}\}$ is a cyclic $2-(v, 3, \lambda)$ design.

The purpose of this paper is to prove the following theorem.

Theorem 1.1. *Let p be a prime with $p \equiv 1(6)$ and let $n \geq 2$ be an integer. There are*

The research on this paper was supported by NTSU research grant number 34845.

isomorphic cyclic $2-(p^n, 3, 1)$ *designs which are not isomorphic by any multiplier.*

This appears to be the first example of such designs. [4]

2. The construction

Throughout this section p is a prime, $p \equiv 1(6)$. Specific examples of the constructions in this section are done in Section 3 for $p = 7$ and 13. The reader is advised to refer to these examples to clarify the constructions.

Lemma 2.1. *For each* $n = 1, 2, 3, \ldots$ *there is an* $\omega_n \in Z_{p^n}$ *such that* $\omega_n \neq 1$ *and* $\omega_n^3 = 1$. *Once a choice is made for* ω_1 *the condition* $\omega_{n-1} \equiv \omega_n \ (p^{n-1})$ *uniquely determines* ω_n. *Furthermore,* $1 + \omega_n + \omega_n^2 = 0$.

Proof. Gauss' Theorem states that the multiplicative units in Z_{p^n} form a cyclic group of order $p^n - p^{n-1} = p^{n-1}(p-1) \equiv 0(3)$. Therefore, there are exactly two elements in Z_{p^n} having multiplicative order 3 and reduction mod p gives the two elements of Z_p of order 3. Furthermore, since $0 = 1 - \omega_n^3 = (1 - \omega_n)(1 + \omega_n + \omega_n^2)$ and $\omega_n \not\equiv 1(p)$, $1 + \omega_n + \omega_n^2 = 0$. □

Let ξ be a primitive root of 1 in Z_p. That is $\xi^{p-1} = 1$ and $\xi^k \neq 1$ for $0 < k < p-1$. Let $\omega_1 = \xi^{(p-1)/3}$. Note that ω_1 has order 3 in Z_p. The difference family $\mathcal{B}_1$ is defined by $\mathcal{B}_1 = \{(\xi^i, \xi^i\omega_1, \xi^i\omega_1^2) \mid 0 \leq i < p - 1/6\}$. It is easily checked that $\mathcal{B}_1$ is a difference family giving a $2-(p, 3, 1)$ cyclic design.

Inductively, for each $n \geq 2$ two difference families are constructed giving $2-(p^n, 3, 1)$ cyclic designs. If $a \in Z_{p^{n-1}}$ we abuse notation and think of $a \in Z$ or Z_{p^n} by using the smallest positive integer equivalent to a mod p^{n-1}. Inductively difference families $\mathcal{B}_n$ and $\mathcal{B}_n'$ are defined on Z_{p^n} by

$$\begin{aligned}\mathcal{B}_n = \{&(ap, bp, cp) \mid (a, b, c) \in \mathcal{B}_{n-1}\}\\ &\cup \{a(1+p^{n-1})(1-2ip^{n-1}),\ a\omega_n(1+p^{n-1})(1-2ip^{n-1}),\ a\omega_n^2(1+p^{n-1})\\ &\times (1-2ip^{n-1}) \mid (a, b, c) \in \mathcal{B}_{n-1},\ a \equiv 0(p),\ i \in Z_p\}\end{aligned}$$

and

$$\begin{aligned}\mathcal{B}_n' = \{&(ap, bp, cp) \mid (a, b, c) \in \mathcal{B}_{n-1}\}\\ &\cup \{p^{n-1}a(2j+a) + a,\ p^{n-1}a\omega_n(2j + a(2+\omega_n))\\ &+ a\omega_n,\ p^{n-1}a\omega_n^2(2j - a\omega_n^2) + a\omega_n^2) \mid (a, b, c) \in \mathcal{B}_{n-1},\ a \not\equiv 0(p),\ j \in Z_p\}.\end{aligned}$$

Note that ω_n is as in Lemma 2.1 with the choice of ω_1 given above. Also note that each triple in $\mathcal{B}_n$ is of the form $(a, a\omega_n, a\omega_n^2)$ or (ap, bp, cp).

Lemma 2.2. *Let $x \in Z_{p^n}$ with $x \not\equiv 0(p)$. Then x occurs in a triple of $\mathcal{B}_n$ if and only if the reduction of $x \bmod p$ occurs in a triple of $\mathcal{B}_1$.*

Proof. The proof is by induction on n. The case $n = 1$ is obvious. It is sufficient to show (i) if $x \not\equiv 0(p)$ and x occurs in a triple of $\mathcal{B}_{n-1}$ then every element in Z_{p^n} which is equivalent to $x \bmod p^{n-1}$ occurs in $\mathcal{B}$ and (ii) for each $y \in Z_{p^n}$ with $y \not\equiv 0(p)$ which occurs in a triple of $\mathcal{B}_n$ there is an $x \in Z_{p^{n-1}}$ with $x \equiv y(p)$ which occurs in a triple of $\mathcal{B}_{n-1}$.

Let $x \in (a, a\omega_{n-1}, a\omega_{n-1}^2) \in \mathcal{B}_{n-1}$ with $x \not\equiv 0(p)$. Note that

$$a\omega_n^j(1+p^{n-1})(1-2ip^{n-1}) \equiv a\omega_{n-1}^j(p^{n-1}) \quad \text{for any } i \in Z_p \quad \text{and} \quad j \in Z_3. \tag{1}$$

Furthermore, note that $1-2ip^{n-1} \equiv (1-2ip^{n-1})^i(p^n)$ and $(1-2p^{n-1})$ has order p in the multiplicative units of Z_{p^n}. Thus as i ranges through Z_p the value of $a\omega^j(1+p^{n+1})(1-2ip^{n-1})$ ranges through all p elements of Z_{p^n} which are equivalent to $a\omega^j \bmod p^{n-1}$. Thus every element of Z_{p^n} equivalent to $x \bmod p^{n-1}$ occurs in a triple of $\mathcal{B}_n$.

Note that Eq. (1) also implies that if $y \in Z_{p^n}$ with $y \not\equiv 0(p)$ and y occurs in a triple of $\mathcal{B}_n$ there is an $x \in Z_{p^{n-1}}$ with $x \equiv y(p)$ such that x occurs in a triple of $\mathcal{B}_{n-1}$. □

Lemma 2.3. *For every $n \geq 1$, $\mathcal{B}_n$ is a difference family.*

Proof. Since $1 + \omega_n + \omega_n^2 = 0$, for each $(a, b, c) \in \mathcal{B}_n$, $a + b + c = 0$. The other condition for a difference family is proved by induction on n. It is easy to check $\mathcal{B}_1$ is a difference family. Let $x \in Z_{p^n} - \{0\}$. If $x \equiv 0(p)$ either x or $-x$ occurs in a triple of $\mathcal{B}_n$ since inductively $\mathcal{B}_{n-1}$ is a difference family. Next suppose $x \not\equiv 0(p)$ and x does not occur in a triple of $\mathcal{B}_n$. Then in $\mathcal{B}_{n-1}$ there are no triples having an entry equivalent to $x \bmod p$. Since $\mathcal{B}_{n-1}$ is a difference family and by Lemma 2.2 every $z \equiv -x(p)$ occurs in a triple of $\mathcal{B}_{n-1}$. Lemma 2.2 then implies $-x$ occurs in $\mathcal{B}_n$. Thus for any $x \in Z_{p^n} - \{0\}$ either x or $-x$ occurs in a triple of $\mathcal{B}_n$. An easy induction shows that the total number of entries in all the triples of $\mathcal{B}_n$ is $(p^n - 1)/2$. Thus for each $x \in Z_{p^n} - \{0\}$ the total number of occurrences of x and $-x$ in triples of $\mathcal{B}_n$ must be exactly 1. □

Lemma 2.4. *For each $n \geq 2$, $\mathcal{B}_n'$ is a difference family.*

Proof. The lemma follows easily from Lemmas 2.2 and 2.3 using the definition of $\mathcal{B}_n'$. □

Since $\mathcal{B}_n$ and $\mathcal{B}_n'$ are difference families $\tilde{\mathcal{B}}_n$ and $\tilde{\mathcal{B}}_n'$ are cyclic designs having the same parameters, $2-(p^n, 3, 1)$. To prove Theorem 1.1 it is sufficient to show

that $\tilde{\mathcal{B}}_n$ and $\tilde{\mathcal{B}}'_n$ are isomorphic designs but are not isomorphic by any multiplier. One isomorphism is the map $\alpha: Z_{p^n} \to Z_{p^n}$ given by $\alpha(x) = p^{n-1}x^2 - (p^{n-1}-1)x$.

Lemma 2.5. *Let α be the map defined above with $n \geq 2$. Then*

(1) *α is bijective,*

(2) *$x \equiv y(p)$ implies $\alpha(y) - \alpha(x) = y - x$,*

(3) *$x \equiv \alpha(x) \bmod p^{n-1}$, and*

(4) *$\alpha(x+h) - \alpha(x) = 2p^{n-1}xh + p^{n-1}h^2 - (p^{n-1}-1)h$.*

Proof. Statements (3) and (4) are easily checked.

Suppose $x = y + kp$. Then $\alpha(x) = p^{n-1}(y+kp)^2 - (p^{n-1}-1)(y+kp) = p^{n-1}y^2 - (p^{n-1}-1)y + kp$. Thus $\alpha(y) - \alpha(x) = -kp = y - x$, and (2) holds.

Suppose $\alpha(x) = \alpha(y)$. Condition (3) implies $x \equiv y \bmod p^{n-1}$. Condition (2) implies $x = y$. Since α is injective it is also surjective. □

Lemma 2.6. *The cyclic designs $\tilde{\mathcal{B}}_n$ and $\tilde{\mathcal{B}}'_n$ are isomorphic for $n \geq 2$ by the map α.*

Proof. It is sufficient to show that for any $(t, s, r) \in \mathcal{B}_n$, $\{\alpha(x), \alpha(x+t), \alpha(x+t+s)\} \in \tilde{\mathcal{B}}'_n$ for any $x \in Z_{p^n}$. Therefore, it would suffice to show $(\alpha(x+t) - \alpha(x), \alpha(x+t+s) - \alpha(x+t), \alpha(x) - \alpha(x+t+s)) \in \mathcal{B}'_n$. First suppose $t \equiv 0(p)$. Then $t \equiv s \equiv r \equiv 0(p)$ and by part (2) of Lemma 2.5, $(\alpha(x+t) - \alpha(x), \alpha(x+t+s) - \alpha(x+t), \alpha(x) - \alpha(x+t+s)) = (t, s, r) \in \mathcal{B}'_n$. Next suppose $t \not\equiv 0(p)$. Then $t = a(1+p^{n-1})(1-2ip^{n-1})$, $s = a\omega_n(1+p^{n-1})(1-2ip^{n-1})$, and $r = a\omega_n^2(1+p^{n-1})(1-2ip^{n-1})$ for some $(a, b, c) \in \mathcal{B}_{n-1}$ and some $i \in Z_{p^n}$. By Lemma 2.5 part 4,

$$\begin{aligned}
(1)\ \alpha(x+t) - \alpha(x) &= 2p^{n-1}xa(1+p^{n-1})(1-2ip^{n-1}) \\
&\quad + p^{n-1}a^2(1+p^{n-1})^2(1-2ip^{n-1})^2 \\
&\quad - (p^{n-1}-1)a(1+p^{n-1})(1-2ip^{n-1}) \\
&= p^{n-1}a(2(x-i)+a) + a
\end{aligned}$$

$$\begin{aligned}
(2)\ \alpha(x+t+s) - \alpha(x+t) &= 2p^{n-1}(x+t)s + p^{n-1}s^2 - (p^{n-1}-1)s \\
&= p^{n-1}a\omega_n(2(x-i) + a(2+\omega_n)) + a\omega_n
\end{aligned}$$

$$\begin{aligned}
(3)\ \alpha(x) - \alpha(x+t+s) &= -(\alpha(x+t+s) - \alpha(x)) \\
&= -(2p^{n-1}x(t+s) + p^{n-1}(t+s)^2 - (p^{n-1}-1)(t+s)) \\
&= p^{n-1}a\omega_n^2(2(x-i) - a\omega_n^2) + a\omega_n^2.
\end{aligned}$$

Therefore, $\{\alpha(x), \alpha(x+t), \alpha(x+t+s)\} \in \tilde{\mathcal{B}}'_n$. □

Lemma 2.7. *There is no multiplier isomorphism from $\tilde{\mathcal{B}}_n$ to $\tilde{\mathcal{B}}'_n$.*

Proof. Suppose $x \to dx$ is a design isomorphism from $\tilde{\mathcal{B}}_n$ to $\tilde{\mathcal{B}}'_n$ where d is a unit

in Z_{p^n}. Then $B = \{d \cdot 0, da(1+p^{n-1})(1-2ip^{n-1}), \quad da(1+\omega_n)(1+p^{n-1})(1-2ip^{n-1})\} \in \bar{\mathcal{B}}'_n$. Note that any of the six possible orderings of the three elements of B give a difference set (t, r, s) with $t \not\equiv 0(p)$, $r = \omega_n^i t$, $s = \omega_n^i r$, and $t = \omega_n^i s$ for $i = 1$ or $i = 2$. We can assume the ordering of the entries of B is taken to give a triple (t, r, s) as in the definition of $\bar{\mathcal{B}}'_n$. First note that

$$r - \omega_n t = p^{n-1}a\omega_n[2j + a(2+\omega_n) - 2j - a] = -p^{n-1}a^2 \neq 0.$$

Also, note that

$$\begin{aligned} r - \omega_n^2 t &= p^{n-1}a\omega_n(2j + a(2+\omega_n)) + a\omega_n - p^{n-1}a\omega_n^2(2j+a) - a\omega_n^2 \\ &\equiv a\omega_1(1-\omega_1) \qquad (p) \\ &\not\equiv 0 \qquad\qquad\quad (p). \end{aligned}$$

Thus $r \neq \omega_n t$ and $r \neq \omega_n^2 t$. This contradicts the condition stated about the triple (t, r, s). Therefore there is no multiplier isomorphism from $\bar{\mathcal{B}}_n$ to $\bar{\mathcal{B}}'_n$. □

Note that Lemma 2.6 and 2.7 together prove Theorem 1.1.

3. Special cases

In this section we do the construction of Section 2 with $p = 7$ and $n = 2$. These designs were first discovered by a computer search of cyclic Steiner triple systems having multiplier automorphisms. The idea of the search was to find a cyclic design with $v = p^2$ that also has the linear function $s(x) = (p+1)x + 1$ as an automorphism. It is easy to see that s has order p^2, and the design has s and translation by 1 as full p^2-cycle automorphisms. An IBM PC programmed in Pascal was used to search for all such Steiner triple systems with $p = 7$ and 13. After the designs were found it was easy to verify that pairs were isomorphic but not by any multiplier map.

For the case $p = 7$, the difference family $\mathcal{B}_1$ is $(1, 2, 4)$ since $2^3 \equiv 1 \bmod 7$. Furthermore, $\omega_2 = 30$ since $30 \equiv 2 \bmod 7$ and $30^3 \equiv 1 \bmod 49$. In the notation of Section 2, the only value for a is 1. Thus $\mathcal{B}_2$ consists of the triple $7 \cdot 1, 7 \cdot 2, 7 \cdot 4) = (7, 14, 28)$ together with triples of the form $(8 \cdot (1 - 14i), 30 \cdot 8 \cdot (1 - 14i), 18 \cdot 8 \cdot (1 - 14i))$ for $i = 0, 1, \ldots, 6$. (All numbers read mod 49.) Thus $\mathcal{B}_2 = \{(7, 14, 28), (8, 44, 46), (43, 16, 39), (29, 37, 32), (15, 9, 25), (1, 30, 18), (36, 2, 11), (22, 23, 4)\}$. On the other hand, $\mathcal{B}'_2$ consists of the triple $(7, 14, 28)$ together with triples of the form $(7 \cdot (2j+1) + 1, 7 \cdot 30 \cdot (2j + 2 + 30) + 30, 7 \cdot 18 \cdot (2j - 18) + 18) = (14j + 8, 28j + 37, 7j + 4)$ where j ranges from 0 to 6. Thus $\mathcal{B}'_2 = \{(7, 14, 28), (8, 37, 4), (22, 16, 11), (36, 44, 18), (1, 23, 25), (15, 2, 32), (29, 30, 39)\}$. An isomorphism from $\bar{\mathcal{B}}_2$ to $\bar{\mathcal{B}}'_2$ is given by $\alpha(x) = 7x^2 - 6x$.

For the case $p = 13$, $\xi = 2$ and $\omega_1 = 2^4 = 3$. Thus $\mathcal{B}_1 = \{(1, 3, 9), (2, 6, 18)\}$.

The difference families for $\mathcal{B}_2$ and $\mathcal{B}_2'$ are mod $13^2 = 169$. The value of ω_2 is 146 since $146^3 \equiv 1 \bmod 169$ and $146 \equiv 3 \bmod 13$. Furthermore, the value of ω_2^2 is 22. $\mathcal{B}_2$ consists of the triples (13, 39, 117) and (26, 78, 65) together with triples of the form $(a \cdot 14 \cdot (1-26i),\ a \cdot 146 \cdot 14 \cdot (1-26i),\ a \cdot 22 \cdot 14 \cdot (1-26i))$ where $a = 1, 2$ and $i = 0, 1, 2, \ldots, 12$. The triples for $\mathcal{B}_2'$ are (13, 39, 117), (26, 78, 65), and triples of the form $(13 \cdot a \cdot (2j+a)+a,\ 13 \cdot a \cdot 146 \cdot (2j + a(2+146)) + a \cdot 146,\ 13 \cdot a \cdot 22 \cdot (2j - a \cdot 22) + a \cdot 22) = (26aj + 13a^2 + a,\ 78aj + 26a^2 + 146a,\ 65aj + 130a^2 + 22a)$ for $a = 1, 2$ and $j = 0, 1, 2, \ldots, 12$. Therefore, $\mathcal{B}_2 = \{(13, 39, 117), (26, 78, 65), (14, 16, 139), (157, 107, 74), (131, 29, 9), (105, 120, 113), (79, 42, 48), (53, 133, 152), (27, 55, 87), (1, 146, 22), (144, 68, 126), (118, 159, 61), (92, 81, 165), (66, 3, 100), (40, 94, 35), (28, 32, 109), (145, 45, 148), (93, 58, 18), (41, 71, 57), (158, 84, 96), (106, 97, 135), (54, 110, 5), (2, 123, 44), (119, 136, 83), (67, 149, 122), (15, 162, 161), (132, 6, 31), (80, 19, 70)\}$ and $\mathcal{B}_2' = \{(13, 39, 117), (26, 78, 65), (14, 3, 152), (40, 81, 48), (66, 159, 113), (92, 68, 9), (118, 146, 74), (144, 55, 139), (1, 133, 35), (27, 42, 100), (53, 120, 165), (79, 29, 61), (105, 107, 126), (131, 16, 22), (157, 94, 87), (54, 58, 57), (106, 45, 18), (158, 32, 148), (41, 19, 109), (93, 6, 70), (145, 162, 31), (28, 149, 161), (80, 136, 122), (132, 123, 83), (15, 110, 44), (67, 97, 5), (119, 84, 135), (2, 71, 96)\}$. An isomorphism between $\mathcal{B}_2$ and $\mathcal{B}_2'$ is given by the formula $\alpha(x) = 13x^2 - 12x$.

References

[1] S. Bays, Sur les systèmes cycliques de triples de Steiner differents pour N premier (où puissance de nombre premier) de la forme $6n+1$, I, Comment. Math. Helv. 2 (1930) 294–305. II–VI, Comment. Math. Helv. 3 (1931) 22–41, 122–147, 307–325.

[2] N.E. Brand and W.C. Huffman, Topological invariants of 2-designs arising from difference families, J. Combinatorial Theory, Series A 36 (1984) 253–278.

[3] N. Brand, Isomorphic designs that are not multiplier equivalent, preprint.

[4] M.J. Colbourn, Algorithmic aspects of combinatorial designs: A survey, Annals of Disc. Math. 26 (1985) pp. 67–136.

[5] P. Lambossy, Sur une manière de differencier les fonctions cycliques d'une forme donnée, Comment. Math. Helv. 3 (1931) 69–102.